

REMARKS

Claims 1-32 are pending in the present application. Claims 1, 9, 11, 12, 14, 15, 20, 28, 30, 31 and 32 were amended; claims 3 and 22 were cancelled. Reconsideration of the claims is respectfully requested.

I. 35 U.S.C. § 112, Second Paragraph, Claims 3 and 22

The examiner has rejected claims 3 and 22 under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter, which applicants regard as the invention. This rejection is respectfully traversed.

In particular, the Examiner has rejected claims 3 and 22 for including the trademarked term "Java". As claims 3 and 22 have been canceled, the objection is moot.

II. 35 U.S.C. § 102, Anticipation, Claims 1-14 and 20-32

The examiner has rejected claims 1-14 and 20-32 under 35 U.S.C. § 102 as being anticipated by *Cane et al.* (US Patent no 5,940,507). This rejection is respectfully traversed.

With regard to claims 1-3, 5, 12, 20-22, 24 and 32, the Examiner stated:

With regard to claims 1-3, 5, 12, 20-22, 24 and 32, as best understood, Cane discloses a method for managing access to data in a processing system (column 1 lines 17-19) including receiving a request for key encrypted data, determining whether the requestor is trusted, and sending the decrypted data (column 4 lines 16-37).

(Office Action, dated July 19, 2004, pages 2-3).

A prior art reference anticipates the claimed invention under 35 U.S.C. § 102 only if every element of a claimed invention is identically shown in that single reference, arranged as they are in the claims. *In re Bond*, 910 F.2d 831, 832, 15 U.S.P.Q.2d 1566, 1567 (Fed. Cir. 1990). Anticipation focuses on whether a claim reads on the product or process a prior art reference discloses, not on what the reference broadly teaches. *Kalman v. Kimberly-Clark Corp.*, 713 F.2d 760, 218 U.S.P.Q. 781 (Fed. Cir. 1983). The *Cane* reference cited by the Examiner does not anticipate the present invention as recited in amended claim 1, because *Cane* fails to teach each and every element of the claim.

Amended independent claim 1, which is representative of amended independent claims 20 and 32 with regard to similarly recited subject matter, reads as follows:

1. A method in a data processing system for managing access to data in a keystore, the method comprising:
 - receiving a request for access to an item of data from a requestor, wherein the item of data is encrypted using a first key;
 - determining whether the requestor is a trusted requestor, wherein the determining step is performed by checking a requestor's identity against a trusted codebase;
 - responsive to a determination that the requestor is a trusted requestor, decrypting a copy of the item of data using a second key to form a decrypted item of data; and
 - sending the decrypted item of data to the requestor.

Claim 1 of the present invention recites the feature of determining whether the requestor is a trusted requestor, wherein the determining step is performed by checking a requestor's identity against a trusted codebase. The Examiner points to the following passage in *Cane* as teaching this feature:

Upon receipt of the encrypted file 20 and the encrypted key 24, the archive server 30 writes the encrypted file 32 to a magnetic tape 36, or other medium or long term storage which is inexpensive and which need not encompass real time access, via tape drive 34 at step 120. The encrypted key 38 is then written to a tape index file 40 at step 122, thereby associating the magnetic tape volume 36 with the encrypted file 32 and the encrypted key 38. In alternative embodiments, a further encryption operation may be performed at the archive server on the encrypted file 32 or the encrypted key 38 to add an additional layer of security.

Recovery of a file is accomplished by the archive server referencing the index to obtain the encrypted key and the volume of the encrypted file. The encrypted file is then retrieved from the volume, and both the encrypted key and the encrypted file are transmitted back to the client. The client then recovers the file through the same two stage process used to encrypt. First, the secondary key must be recovered by decrypting the encrypted key with the master. Second, the original file may be recovered by decrypting the encrypted file with the secondary key.

(*Cane*, col. 4, lines 16-37)

The passage above teaches that an archive server receives an encrypted file and an encrypted key. The archive server stores the encrypted file in a storage medium, and the encrypted key is written to an index file. Additional encryption operations may also be

performed on the encrypted file or key. When a client wants to access the stored data, the archive server uses the index to obtain the encrypted key and file, and sends them to the client. The client may then use the same two stage process used to encrypt the file (a secondary key is recovered by decrypting the encrypted key with a master key and the original file is recovered by decrypting the encrypted file with the secondary key). Thus, the master key is needed to perform the two stage process, wherein the secondary key is recovered by decrypting the encrypted key with the master key.

However, *Cane* teaches in column 3, line 64 to column 4, line 1 that the master key is retained at the client, as shown in the passage below:

The encrypted file 20 and encrypted key 24 are then transmitted to the archive server at steps 116 and 118, respectively, while the master key 22 is retained at the source system 8 at step 114.

Block 114 in Figure 2 further illustrates that the master key is retained at the client in *Cane*:

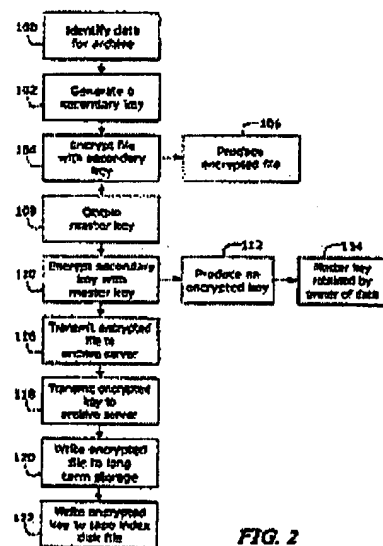


FIG. 2

Thus, as the master key is needed to decrypt the stored data, and as the master key is stored at the data source/client, *Cane* merely teaches that the source client is the only requestor able to decrypt the stored data.

Although *Cane* mentions further encrypting the stored encrypted data or the associated encrypted key at the archive server as a security precaution, there is no

mention in *Cane* of determining whether the requestor is a trusted requestor, wherein the determining step is performed by checking a requestor's identity against a trusted codebase. As the requestor in *Cane* retains the master key which is needed to decrypt the stored data, there is no need in *Cane* to check the client's identity against a trusted codebase. By virtue of having the master key in its possession, the client is ensured that it can recover the stored file. In fact, there is no mention in *Cane* of checking a trusted codebase at all. Rather, *Cane* merely teaches that an originator of the stored encrypted data may recover the stored encrypted data through the same two stage process used originally to encrypt the data. A secondary key is recovered by decrypting the encrypted key with the master key which is retained at the client, and the original file is recovered by decrypting the encrypted file with the secondary key (see *Cane*, col. 4, lines 32-37). Consequently, as *Cane* does not teach checking a trusted codebase to check that the requestor is a trusted requestor, *Cane* does not teach the feature of determining whether the requestor is a trusted requestor, wherein the determining step is performed by checking a requestor's identity against a trusted codebase as recited in claim 1 of the present invention.

Cane also does not teach the feature of decrypting a copy of the item of data using a second key to form a decrypted item of data in response to a determination that the requestor is a trusted requestor as recited in claim 1 of the present invention. The Examiner again points to column 4, lines 16-37 of *Cane* (recited above) as teaching this feature.

The above cited passage of *Cane* teaches decrypting an encrypted key using a master key to form a secondary key. Then the secondary key is used to decrypt the encrypted file. *Cane* teaches only one encrypted file, which is the original file. In contradistinction, the present invention receives a request for a first item of data encrypted with a first key and instead, decrypts a second item of data, which is a copy of the first item of data, using a second key. In other words, the encrypted file in *Cane* is not a copy of an item of data wherein the original item of data is encrypted using a first key and the copy is encrypted with a second, different key, as in claim 1.

Claim 1 of the present invention also recites sending the decrypted item of data to the requestor. The Examiner again points to column 4, lines 16-37 of *Cane* (recited

above) as teaching this feature. However, *Cane* actually teaches that the encrypted data and its associated encrypted key are transmitted, still in their encrypted form, to the requestor/client, who then decrypts the data at the requestor's location. Thus, *Cane* fails to teach sending the decrypted item of data to the requestor as recited in claim 1 of the present invention.

Furthermore, *Cane* does not teach, suggest, or give any incentive to make the needed changes to reach the presently claimed invention. *Cane* actually teaches away from the presently claimed invention because it teaches that the data is stored using a two stage encryption process, involving a master key and a secondary key, whereby the encrypted file and associated encrypted key are stored at an archive server while the original source retains the master key (see *Cane*, col. 3, lines 32-44). Therefore, *Cane* teaches that only the source of the data can decrypt the encrypted data. In contrast, the present invention teaches that the archiving server creates and maintains the keys used to encrypt stored information. Therefore the archiving server has the ability to decrypt the information stored therein, as well as the ability to allow other users to access and manipulate the stored data whether or not the data originated with the particular requesting user. Absent some teaching, suggestion, or incentive to modify *Cane* in this manner, the presently claimed invention can be reached only through an improper use of hindsight using the Applicants' disclosure as a template to make the necessary changes to reach the claimed invention.

Therefore, *Cane* does not teach all the elements of rejected claims 1, 20 and 32. Accordingly, Applicants respectfully submit that claims 1, 20 and 32 are patentable over the *Cane* reference.

Claims 2-10 are dependent claims depending on claim 1. Claims 21-29 are dependent claims depending on claim 20. As Applicants have already demonstrated that independent claims 1 and 20 are patentable over the *Cane* reference, Applicants submit that dependent claims 2-10 and 21-29 are patentable over the *Cane* reference for the same reasons cited in reference to independent claims 1 and 20 and include additional features not found in the *Cane* reference. For example, claim 9 recites the feature of storing an encrypted copy of a new item of data in the keystore. As *Cane* does not teach storing a

copy of an encrypted file, it follows that *Cane* does not teach storing an encrypted copy of a new item of data in the keystore.

In view of the above, Applicants respectfully submit that the rejection of claims 1-10 and 21-29 under 35 U.S.C. § 102 has been overcome.

As for claims 11, 30 and 31, the Examiner stated:

With regard to claims 11, 30 and 31, *Cane* discloses sending the key with the data (column 4 lines 29-31).

(*Office Action*, dated July 19, 2004, page 3). Amended independent claim 11, which is representative of amended independent claims 12, 30, and 31 with regard to similarly recited subject matter, reads as follows:

11. A method in a data processing system for managing access to data in a keystore, the method comprising:
 - receiving a request for access to an item of data from a requestor, wherein the item of data is encrypted using a first key;
 - determining whether the requestor is a trusted requestor, wherein the determining step is performed by checking the requestor's identity against a trusted codebase; and
 - responsive to a determination that the requestor is a trusted requestor, sending a second key and an encrypted copy of the item of data to the requestor.

As mentioned in the response to the rejection of claim 1 above, *Cane* does not teach the feature of determining whether the requestor is a trusted requestor, wherein the determining step is performed by checking a requestor's identity against a trusted codebase.

Additionally, claim 11 recites that in responsive to a determination that a requestor is a trusted requestor, sending a second key, along with an encrypted copy of the item of data to the requestor. The Examiner has cited the following passage of *Cane* as teaching this feature:

The encrypted file is then retrieved from the volume, and both the encrypted file and encrypted key are transmitted back to the client.

(*Cane*, col. 4, lines 29-31).

The passage above teaches sending an encrypted key along with encrypted data back to the requestor. In contrast, the present invention recites sending a second key and an encrypted copy of the item of data to the requestor. As argued above in the rejection to

claim 1, *Cane* does not teach creating or storing a copy of an item of data wherein the original item of data is encrypted using a first key and the copy is encrypted with a second, different key. Instead, *Cane* teaches sending the original, encrypted file to the requestor. Thus, it follows that *Cane* does not teach sending an encrypted copy of the item of data wherein the original item of data is encrypted using a first key and the copy is encrypted with a second, different key.

Furthermore, *Cane* teaches that the secondary key for decrypting the encrypted item of data is also itself decrypted by a master key that is kept by the client (*Cane*, col. 4, lines 32-37). However, *Cane* makes no mention of sending a key to the client with an encrypted copy of the item of data. Rather, the secondary key in *Cane* is sent to the client in an encrypted form along with the original encrypted file. Thus, *Cane* does not teach the feature of sending a second key with an encrypted copy of the item of data to the requestor as recited in claim 11 of the present invention.

Therefore, *Cane* does not teach all the elements of rejected claims 11, 12, 30 and 31. Accordingly, Applicants respectfully submit that claims 11, 30, and 31 are patentable over the *Cane* reference.

Claims 13 and 14 are dependent claims depending on claim 12. Applicants have already demonstrated that independent claim 12 is patentable over the *Cane* reference. Applicants submit that dependent claims 13 and 14 are also patentable over the *Cane* reference at least by virtue of being dependent upon an allowable claim.

In view of the above, Applicants respectfully submit that the rejection of claims 11-14, 30 and 31 under 35 U.S.C. § 102 has been overcome.

III. 35 U.S.C. § 103, Obviousness, Claims 15-19

The examiner has rejected claims 15-19 under 35 U.S.C. § 103 as being unpatentable over *Cane et al.* (US Patent no 5,940,507). This rejection is respectfully traversed.

All limitations of the claimed invention must be considered when determining patentability. *In re Lowry*, 32 F.3d 1579, 1582, 32 U.S.P.Q.2d 1031, 1034 (Fed. Cir. 1994). In comparing *Cane* to the claimed invention to determine obviousness, limitations

of the presently claimed invention may not be ignored. Amended independent claim 15 recites:

15. A data processing system comprising:
a bus system;
a communications unit connected to the bus, wherein data is sent and received using the communications unit;
a memory connected to the bus system, wherein a set of instructions are located in the memory; and
a processor unit connected to the bus system, wherein the processor unit executes the set of instructions to receive a request for access to an item of data from a requestor, wherein the item of data is encrypted using a first key, determine whether the requestor is a trusted requestor, wherein the determining step is performed by checking a requestor's identity against a trusted codebase, and send a second key and an encrypted copy of the item of data to the requestor in response to a determination that the requestor is a trusted requestor.

As shown in the response to the rejections of claims 1 and 11 above, *Cane* still does not teach or suggest all the claim limitations in independent claim 15. *Cane* still does not teach or suggest the feature of determining whether a requestor is a trusted requestor by checking a requestor's identity against a trusted codebase. As a proper obviousness rejection requires that all features of the claims must be taught or suggested in the cited references, Applicants respectfully submit that claim 15 is not obvious in view of *Cane*.

Claims 16-19 are dependent claims depending on claim 15. Applicants have already demonstrated that independent claim 15 is patentable over the *Cane* reference. Applicants submit that dependent claims 16-19 are patentable over the *Cane* reference at least by virtue of being dependent upon an allowable claim.

Therefore, the rejection of claims 15-19 under 35 U.S.C. § 103 has been overcome.

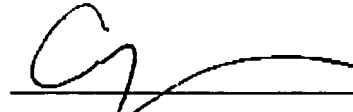
IV. Conclusion

It is respectfully urged that the subject application is patentable over *Cane* and is now in condition for allowance.

The examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

DATE: 10/15/04

Respectfully submitted,



Cathrine K. Kinslow
Reg. No. 51,886
Yee & Associates, P.C.
P.O. Box 802333
Dallas, TX 75380
(972) 367-2001
Attorney for Applicants

CK/bj